FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

10 Tips for Smart Holiday Shopping Online

Going online to shop for the holidays this year? Some of us do it to avoid crowds, some to save gas, and some for the convenience of shopping at any time of day or night. Experts are predicting that consumers will spend more online this holiday season than ever. In fact, a recent Forrester study reports that 11 percent of online shoppers said they would do three-quarters or more of their holiday spending online, translating to an estimated $33 billion in 2007, up from $27 billion in 2006.

The Federal Trade Commission (FTC), the nation's consumer protection agency, and the National Cyber Security Alliance (NCSA), a non-profit organization devoted to cyber security education and awareness, want you to know that scammers follow the money and will be online this holiday season, too. To reduce the risk of a rip-off — and to protect your personal information and your computer from identity thieves and hackers — the FTC and NCSA offer these tips for safer and smarter online shopping this holiday season:

Check out the seller. If you're thinking about shopping on a site with which you're not familiar, do some independent research before you buy.

- If it's your first time on an unfamiliar site, call the seller's phone number, so you know you can reach them if you need to. If you can't find a working phone number, take your business elsewhere.
- Type the site's name into a search engine: If you find unfavorable reviews posted, you may be better off doing business with a different seller.
- Read the site's privacy policy to learn how it uses and shares your personal information.
- Consider using a software toolbar that rates websites and warns you if a site has gotten unfavorable reports from experts and other Internet users. Some reputable companies provide free tools that may alert you if a website is a known phishing site or is used to distribute spyware.

Read return policies. Despite your best intentions, some gifts may need to be returned or exchanged. Before you buy, read the return policy. Some retailers give customers extra time so gifts can be returned or exchanged after the holidays; others give purchasers as little as a week — if they accept returns at all. A number of retailers offer shorter return windows for certain products and some charge "restocking" fees. Find out who covers the shipping cost — the customer or the merchant — on a return or exchange, and if your online purchase can be returned to a brick-and-mortar store.

Know what you're getting. Read the seller's product description closely. Name-brand items at greatly reduced prices could be counterfeit.

Don't fall for a false email or pop-up. Legitimate companies don't send unsolicited email messages asking for your password or login name, or your financial information. But scammers do. In fact, crooks often send emails that look just like they're from legitimate companies — but direct you to

click on a link, where they ask for your personal information. Delete these emails. They're an attempt to get your information and to facilitate identity theft or other crimes. In addition, just clicking a link in a fraudulent email could install spyware on your computer.

Look for signs a site is safe. When you're ready to buy something from a seller you trust, look for signs that the site is secure — such as a closed padlock on the browser's status bar — before you enter your personal and financial information. When you're asked to provide payment information, the beginning of the website's URL address should change from http to shttp or https, indicating that the purchase is encrypted or secured.

Secure your computer. At a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. Security software must be updated regularly to help protect against the latest threats. Set your security software and operating system (like Windows or Apple's OS) to update automatically. Visit OnGuardOnline.gov and staysafeonline.org to learn more about security software, firewalls, and other ways to secure your computer.

Consider how you'll pay. Credit cards generally are a safe option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Also, if your credit card number is stolen, you generally won't be liable for more than $50 in charges. Don't send cash or use a money-wiring service because you'll have no recourse if something goes wrong.

Know the full price, and check out incentives. If you're looking for the best deal, compare total costs, including shipping and handling. The holiday season is prime time for online retailers, and many are offering incentives like free shipping. But some "free" shipping deals may come with strings attached, such as requirements to spend a minimum amount or buy certain products. Consider whether one company offers a more generous return policy. If you use a price comparison site to find a bargain, enter the product's model number, and be as specific as you can about its features.

Keep a paper trail. Print and save records of your online transactions, including the product description and price, the online receipt, and copies of any email you exchange with the seller. Read your credit card statements as soon as you get them to make sure there aren't any unauthorized charges.

Turn your computer off when you're finished shopping. Many people leave their computers running 24/7, the dream scenario for scammers who want to install malicious software on your machine and then control it remotely to commit cyber crime. To be extra safe, switch off your computer when you are not using it.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.